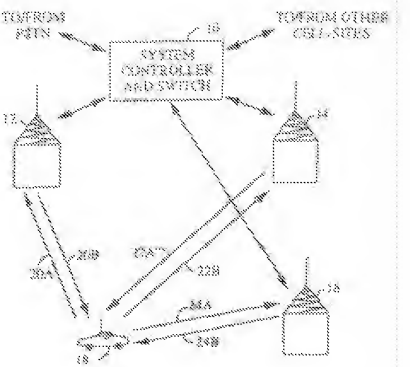
APPARATUS AND METHOD OF USING A CIPHERING KEY IN A HYBRID COMMUNICATIONS NETWORK

Patent number:	JP2005512471 (T)
Publication date:	2005-04-28
Inventor(s):	
Applicant(s):	
Classification:	
- international:	*H04B7/26; H04L9/08; H04L9/14; H04L9/32; H04W12/04; H04W36/12; H04W36/14;* H04B7/26; H04L9/08; H04L9/14; H04L9/32; H04W12/00; H04W36/00; (IPC1-7): H04L9/08; H04L9/14; H04Q7/38
- european:	H04L29/06S6; H04W12/04
Application number:	JP20030552012T 20021205
Priority number(s):	US20010340755P 20011207; US20020350401P 20020117; US20020077502 20020214; US20020358491P 20020219; WO2002US39209 20021205

Abstract not available for JP 2005512471 (T)
Abstract of correspondent: **WO 03051072 (A1)**
Translate this text

A method of using a ciphering key in a mobile station (18) from a first base station (12) in a first cellular communications system controlled by a first mobile switching control (10) station to a second base station in a second, different cellular system controlled by a second mobile switching control station is described. The method comprises generating for the mobile station a cipher key for use by the mobile station during communication in the second cellular communications system. The cipher key is generated by the mobile station from a private key assigned to the mobile station for the second cellular communications system and from a random number generated by the second cellular communications system. The cipher key is then communicated to the first mobile system and a private long code is generated for use by the mobile station during communication in the first cellular communications system.



(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-512471
(P2005-512471A)
(43)公表日　平成17年4月28日(2005.4.28)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601B	5J104
H04L	9/14	H04L	9/00	601E	5K067
H04Q	7/38	H04B	7/26	109R	
		H04B	7/26	109G	
		H04L	9/00	641	

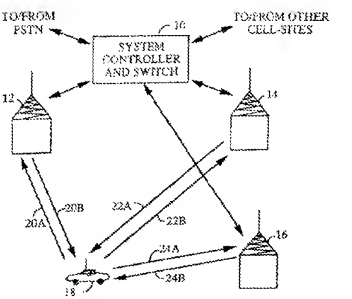
審査請求 未請求　予備審査請求 有　（全 18 頁）

(21)出願番号	特願2003-552012 (P2003-552012)
(86)(22)出願日	平成14年12月5日 (2002.12.5)
(85)翻訳文提出日	平成16年6月7日 (2004.6.7)
(86)国際出願番号	PCT/US2002/039209
(87)国際公開番号	WO2003/051072
(87)国際公開日	平成15年6月19日 (2003.6.19)
(31)優先権主張番号	60/340,755
(32)優先日	平成13年12月7日 (2001.12.7)
(33)優先権主張国	米国(US)
(31)優先権主張番号	60/350,401
(32)優先日	平成14年1月17日 (2002.1.17)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/077,502
(32)優先日	平成14年2月14日 (2002.2.14)
(33)優先権主張国	米国(US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
QUALCOMM INCORPORATED
アメリカ合衆国、カリフォルニア州　92121-1714、サン・ディエゴ、モアハウス・ドライブ　5775
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘
最終頁に続く

(54)【発明の名称】ハイブリッド通信ネットワークで暗号解読用鍵を用いる装置及び方法

(57)【要約】
【課題】ハイブリッド通信ネットワークで暗号解読用鍵を用いる装置及び方法
【解決手段】第１の移動切換制御局（１０）によって制御される第１のセルラー通信システム中の第１の基地局（１２）から第２の移動切換制御局によって制御される第２の別のセルラーシステム中の第２の基地局への暗号解読用鍵を移動局（１８）で用いる方法を説明している。前記方法は、前記第２のセルラー通信システム内での通信中に前記移動局によって用いられる暗号解読鍵を前記移動局に対して生成することを含む。前記暗号解読鍵が、前記第２のセルラー通信システムに対する前記移動局に割り当てられた秘密鍵と前記第２のセルラー通信システムによって発生した乱数とから前記移動局によって生成される。次に、前記暗号解読鍵が前記第１のモバイルシステムに通信され、また、前記第１のセルラー通信システム内での通信中に前記移動局によって用いられる秘密長符号が、前記移動局に対して生成される。



【特許請求の範囲】
【請求項１】
第１の移動切換制御局によって制御される第１のセルラー通信システム中の第１の基地局と第２の移動切換制御局によって制御される第２の別のセルラーシステム中の第２の基地局とから、移動局を有するシステムにおいて、
前記第２のセルラー通信システム内での通信中に前記移動局によって用いられる暗号解読鍵を前記移動局に対して生成することであって、前記暗号解読鍵が、前記第２のセルラー通信システムに対する前記移動局に割り当てられた秘密鍵と前記第２のセルラー通信システムによって発生した乱数とから前記移動局によって生成され、
前記暗号解読鍵を前記第１の移動局に通信し、
前記第１のセルラー通信システム内での通信中に前記移動局によって用いられる秘密長符号を前記移動局に対して生成すること
を備える方法。
【請求項２】
前記第１のシステムは、前記システムと前記移動局間でデータを転送するためのチャネルを備え、
前記暗号解読鍵を前記システムに対して前記データ転送用チャネルを用いて送信することを更に備える請求項１に記載の方法。
【請求項３】
前記チャネルはページングチャネルである、請求項２に記載の方法。
【請求項４】
前記第１のセルラー通信システムは、第１の移動切換制御局によって制御される第１の基地局を備え、前記第２のセルラー通信システムは、第２の移動切換制御局によって制御される第２の基地局を備え、
前記方法は、
前記第１の基地局によって送信される信号のパラメータを前記移動局で測定し、
前記第２の基地局によって送信される信号のパラメータを前記移動局で測定し、
前記パラメータが所定の状態に達したら、信号品質メッセージを前記移動局から前記第１の基地局を介して前記第１の移動切換制御局に対して通信し、
前記第１の移動切換制御局で、チャネル要求メッセージのための情報を前記第２の移動切換制御局に対して生成し、
前記情報を前記第１の移動切換制御局から前記移動局に通信し、
前記移動局で、前記第１の移動切換制御局からの前記情報から、前記第２の移動切換制御局に対するチャネル要求メッセージを生成し、
前記チャネル要求メッセージを前記移動局から前記第２の移動切換制御局に対して通信すること、
を備える請求項１に記載の方法。
【請求項５】
前記第２の移動切換制御局で、前記移動局に対するチャネルを前記第２の通信システム中で識別するチャネル情報を生成することを更に備える、請求項４に記載の方法。
【請求項６】
前記モバイルユニットと前記第２の基地局との間の通信を前記識別されたチャネルで確立することを更に備える、請求項５に記載の方法。
【請求項７】
前記モバイルユニットと前記第１の基地局間の通信を中断することを更に備える、請求項６に記載の方法。
【請求項８】
前記パラメータは信号強度に対応する、請求項４に記載の方法。
【請求項９】
前記第１のセルラー通信システムはＣＤＭＡシステムである、請求項４に記載の方法。

【請求項１０】
前記第２のセルラー通信システムはＧＳＭシステムである、請求項９に記載の方法。
【請求項１１】
セルラー通信システム中の基地局と信号を送受信するように操作可能なトランシーバチェインと、
前記セルラー通信システムによって発生した乱数を受信し、
前記セルラー通信システム内で通信中に前記移動局によって用いられる暗号解読鍵を前記移動局に対して生成するコントローラであって、前記暗号解読鍵は前記第２のセルラー通信システムに対する前記移動局に割り当てられた秘密鍵と前記受信された乱数とから生成されるコントローラと、
を備える移動局。
【請求項１２】
第１の移動切換制御局によって制御される第１のセルラー通信システム中の第１の基地局と第２の移動切換制御局によって制御される第２の別のセルラーシステム中の第２の基地局までを有するシステムにおいて、
前記第２のセルラー通信システム内での通信中に前記移動局によって用いられる暗号解読鍵を前記移動局に対して生成する手段であって、前記暗号解読鍵が、前記第２のセルラー通信システムに対する前記移動局に割り当てられた秘密鍵と前記第２のセルラー通信システムによって発生した乱数とから前記移動局によって生成される手段と、
前記暗号解読鍵を前記第１のモバイルシステムに通信する手段と、
前記第１のセルラー通信システム内での通信中に前記移動局によって用いられる秘密長符号を前記移動局に対して生成する手段と、
を備える装置。
【請求項１３】
前記第１のシステムは、前記システムと前記移動局間でデータを転送するためのチャネルを備え、
前記暗号解読鍵を前記システムに対して前記データ転送用チャネルを用いて送信する手段を更に備える請求項１２に記載の装置。
【請求項１４】
前記チャネルはページングチャネルである、請求項１３に記載の装置。
【請求項１５】
前記第１のセルラー通信システムはＣＤＭＡシステムである、請求項１２に記載の装置。
【請求項１６】
前記第２のセルラー通信システムはＧＳＭシステムである、請求項１５に記載の装置。
【発明の詳細な説明】
【関連出願】
【０００１】
本出願は、２００１年１２月７日に提出された出願番号第６０／３４０，７５５号の「様々なセルラー通信システム同士間でのハンドオフを達成させる方法及び装置（Method and Apparatus for Effecting Handoff Between Different Cellular Communications Systems）」という題名の米国仮特許出願の優先権を請求し、また、２００２年２月１４日に提出された出願番号第１０／０７７，５０２号の「様々なセルラー通信システム同士間でのハンドオフを達成させる方法及び装置（Method and Apparatus For Effecting Handoff Between Different Cellular Communications Systems）」という題名の米国特許出願と、２００２０年２月１７日に提出された出願番号第６０／３５０，４０１号の「ＧＳＭ－１ｘＭＳＣを用いたＣＤＭＡ　１ｘネットワークにおけるＧＳＭ認証、暗号化及び他の機能サポート（GSM Authentication, Encryption and Other Feature Support in a CDMA 1x Network Using a GSM-1x MSC）」という題名の米国仮特許出願の優先権を請求するものである。

【技術分野】
【０００２】
本発明は一般的に、暗号解読用鍵を用いる方法及び装置に関する。
【背景技術】
【０００３】
いわゆる符号分割多元接続（ＣＤＭＡ）変調技術は、非常に多くのシステムユーザが存在する通信をし易くするためのいくつかある技術のうちの１つにすぎない。時分割多元接続方式（ＴＤＭＡ）、周波数分割多元接続方式（ＦＤＭＡ）及び、振幅圧伸単側波帯（ＡＣＳＳＢ）などのＡＭ変調方式などの他の技術も利用可能であるとはいえ、ＣＤＭＡ方式はこれら他の変調技術にない重要な長所を有している。多元接続通信システムでＣＤＭＡ方式を使用することは、本譲受人に譲受され、その開示が参照してここに組み込まれる「衛星中継器又は地上リピータを用いるスペクトル拡散多元接続通信システム（Spread Spectrum Multiple Access Communication System Using Satellite Or Terrestrial Repeaters）」という題名の米国特許第４，９０１，３０７号に開示されている。
【０００４】
米国特許第４，９０１，３０７号には、各々がトランシーバを持っている非常に多くのモバイル電話システムのユーザが、符号分割多元接続（ＣＤＭＡ）スペクトル拡散通信信号を用いて衛星中継器又は地上局（セル基地局又はセルサイトとしても知られている）を介して通信する多元接続技術が記載されている。ＣＤＭＡ通信を利用するに際して、周波数スペクトルを何回も再使用して、システムユーザの容量を増加させることが可能である。ＣＤＭＡ技術を用いると、その結果、他の多元接続技術の使用によって達成されるより遙かに高いスペクトル効率が得られる。
【０００５】
従来のセルラー電話システムでは、利用可能な周波数帯域は、アナログＦＭ変調技術を用いる限り、一般的に３０ｋＨｚという帯域幅のチャネルに分割される。システムサービスのエリアは、地理的に、様々に変わるサイズのセルに分割される。利用可能な周波数チャネルは、各々が通常は等しい数のチャネルを含む複数のセットに分割される。この周波数のセットは、他局間干渉の可能性を最小化するようにセルに割り当てられる。例えば、７個の周波数セットが存在し、セルは等しいサイズの六角形であるようなシステムを考える。１個のセルで用いられる周波数セットはそのセルの隣接する、すなわち、これを取り囲む６個のセル中では用いられない。更に、１個のセル中での周波数セットは、次に最も近くに隣接している１２個のセルでは用いられない。
【０００６】
従来のセルラーシステムでは、実施されるハンドオフ方式は、移動局が２個のセル間の境界を越境する際に呼出し又は他のタイプの接続（すなわちデータリンク）の継続を許可することを意図するものである。１つの呼出しから他の呼出しへのハンドオフは、この呼出し又は接続を取り扱っているセル基地局中の受信器が、移動局からの受信信号強度が所定のしきい値未満に落ちたことに気付くと開始される。低信号強度表示は、移動局がセル境界の近くにいなければならないことを暗示する。信号レベルが所定のしきい値未満に落ちると、基地局は、システムコントローラに対して、隣の基地局が現行の基地局より良好な信号強度を持つ移動局信号を受信しているかを判定するように要請する。
【０００７】
システムコントローラは、現行の基地局の照会に応答して、ハンドオフ要求のメッセージを隣の基地局に送る。現行の基地局に隣接する基地局では、指定されたチャネル上の移動局からの信号を探索する特殊スキャニング受信器を用いる。隣接する基地局のうちの１つでも適切な信号レベルをシステムコントローラに報告すると、ハンドオフが試行される。
【０００８】
次に、ハンドオフは、新しい基地局中で用いられているチャネルセットのうちの空きチャネルが選択されると開始される。制御メッセージが移動局に送られて、それに対して、

現行のチャネルから新しいチャネルに切換わるように指令する。同時に、システムコントローラは、呼出しを第１の基地局から第２の基地局に切換える。

【０００９】

従来のシステムでは、新しい基地局へのハンドオフが不成功の場合、呼出しは中断される。ハンドオフの失敗が発生するには多くの理由がある。呼出しを通信するために利用可能な空きチャネルが隣接するセル中にないと、ハンドオフは失敗する。当該移動局が聞こえると別の基地局が報告する場合もまた、ハンドオフは失敗するが、事実、この基地局では、完全に違うセル中の同じチャネルを用いている別の移動局が聞こえる。この報告エラーの結果、呼出しは間違ったセル、一般的には、信号強度が通信を維持するには不十分であるようなセルに切換えられる。更に、移動局がチャネル切換コマンドの聞き取りに失敗すると、ハンドオフは失敗する。実際に操作した経験によると、システムの信頼性に疑問を投げかけるようなハンドオフの失敗は、頻繁に発生する。

【００１０】

従来の電話システムにおける別の一般的問題は、移動局が２個のセルの境界の近くに存在する場合に発生する。この状況下では、信号レベルは、双方の基地局で変動する傾向がある。この信号レベルの変動の結果、「ピンポン」状況、すなわち要求が繰り返されて、呼出しが２つの基地局間で行ったり来たりするという状況が発生する。このような更なる不必要なハンドオフ要求のため、移動局が、チャネル切換コマンドを不正確に聞き取ったり、コマンドが全く聞こえなかったりする可能性が増す。更に、ピンポン状況のため、全てのチャネルが現在使用中であり、ハンドオフを受け入れるためには利用不可能であるようなセルに呼出しが不注意に転送されると、このシステム呼出しが中断される可能性が増す。

【００１１】

その開示内容が参照してここに組み込まれる、本譲受人に譲受された「ＣＤＭＡセルラー電話システム中で通信中にソフトハンドオフを提供する方法及びシステム（Method and System For Providing A Soft Handoff In Communications In A CDMA Cellular Telephone System）」という題名の米国特許第５，１０１，５０１号には、ハンドオフ中に２つ以上のセル基地局を介して移動局と通信する方法及びシステムが開示されている。この環境下では、セルラーシステム内での通信は、移動局が脱出しようとしているセルに対応する基地局から、移動局が入ろうとしているセルに対応する基地局への結果として起こるハンドオフによっては中断されない。このタイプのハンドオフは、モバイルによるセル基地局同士間の通信における「ソフトな」ハンドオフと考えられるが、この場合、２つ以上の基地局又はセクターの基地局が同時に移動局に送信する。このような「ソフトな」ハンドオフ技術を用いると、繰り返されるハンドオフ要求が対を成す基地局同士間で成されるピンポン状況の発生率を大幅に減少させることが分かっている。

【００１２】

改良されたソフトハンドオフ技術が、本譲受人に譲受され、その開示内容が参照してここに組み込まれる「ＣＤＭＡセルラー通信システムにおける移動局支援のソフトハンドオフ（Mobile Station Assisted Soft Handoff In A CDMA Cellular Communications System）」という題名の米国特許第５，２６７，２６１号内に開示されている。このソフトハンドオフ技術は、システム内の各基地局によって送信される「パイロット」信号の強度を移動局で測定する点が改良されている。このパイロット強度測定のため、実行可能な基地局ハンドオフ候補が識別し易くなることによって、ソフトハンドオフ処理の助けとなる。

【００１３】

この改良型ソフトハンドオフ技術は、移動局が隣接する基地局からのパイロットの信号強度を監視することを規定する。測定された信号強度が所定のしきい値を超えると、移動局は、移動局が通信している基地局を介して信号強度メッセージをシステムコントローラに対して送る。システムコントローラから新しい基地局と前記移動局へのコマンドメッセージによって、これら新しい基地局と現行の基地局とを介して同時発生通信が確立される。移動局が通信している基地局のうちの少なくとも１つに対応するパイロットの信号強度

が所定のレベル未満に落ちたことを移動局が検出すると、移動局は、対応する基地局の測定された信号強度測定値をシステムコントローラに対して、それが通信している基地局を介して報告する。システムコントローラから識別された基地局と移動局へのコマンドメッセージによって、対応する基地局を介しての通信が終了し、一方、その他の１つ以上の基地局を介しての通信は継続される。

【００１４】

前述の技術は同じセルラーシステム内のセル同士間の呼出し転送に良好に適しているとはいえ、別のセルラーシステムからの基地局のサービスを受けているセル中に移動局が入ってくることによってより困難な状況が提示される。このような「システム間」ハンドオフにおける１つの複雑化要因は、隣のセルラーシステムがしばしば異質な特徴を有することである。例えば、隣接するセルラーシステムは、頻繁に違う周波数で動作し、また、その多くが、互いに異なったレベルの基地局出力やパイロット強度を維持している。このような相違によって、移動局は、既存のモバイル支援式ソフトハンドオフ技術によって想定されるパイロット強度の比較や類似の操作を実行することが事実上不可能となる。

【００１５】

システム間ソフトハンドオフを実行するためにリソースが利用不可能な場合、サービスを継続したければ、１つのシステムから別のシステムへの呼出し又は接続のハンドオフのタイミングは重要である。すなわち、システム間ハンドオフは、システム間での呼出し又は接続の転送が最も成功しそうな時点で実行しなければならない。本明細書ではハードハンドオフと呼ばれるこのようなハンドオフにおいては、移動局と一方のシステム間での通信は、移動局と他方のシステム間での通信が開始可能となる以前に停止しなければならない。その結果、例えば、

（ｉ）空きチャネルが新しいセルで利用可能である場合と、

（ｉｉ）移動局が実際に新しいセル基地局の範囲内にあるが、それは現行のセル基地局とのコンタクトを失っていない場合と、

（ｉｉｉ）移動局が、チャネル切換コマンドが受信されることが保証されている位置に存在する場合、

にだけハンドオフを試行すべきである。

【００１６】

このようなシステム間ハードハンドオフは、互いに異なったシステムの基地局同士間で「ピンポン」ハンドオフ要求が成される可能性が最小となるように実行されるのが理想的である。しかしながら、いつ、そしてどの基地局を介して、移動局が新たな周波数とチャネルの情報を供給され、既存の呼出しや接続を転送するように命令されるかを識別する既存のハンドオフ手順が失敗するため困難となる。

【００１７】

既存のシステム間ハンドオフ技術の上記の欠点及び他の欠点のため、セルラー通信の品質が劣化し、競合するセルラーシステムが増え続けるに連れて性能が更に劣化する。従って、その結果、互いに異なったセルラー通信システムの基地局同士間での呼出しや接続のハンドオフを信頼性高く指揮することが可能なシステム間ハンドオフ技術に対する必要性が存在する。

【００１８】

本譲受人に譲受され、その開示内容が参照してここに組み込まれる「ＣＤＭＡセルラー通信システムにおける移動局支援式ソフトハンドオフ（Mobile Station Assisted Soft Handoff In A CDMA Cellular Communications System）」という題名の米国特許第５，６９７，０５５号には、第１と第２のセルラーシステムの基地局同士間での移動局による通信のシステム間ハンドオフを実行する方法及びシステムが記載されている。移動局では、第２のシステムの第２の基地局によって送信された信号の定量化可能パラメータが測定される。この定量化可能パラメータの測定値が第１の所定のレベルを越えると、移動局は信号品質メッセージを第１のシステムの第１の基地局を介して第１の移動切換制御局に通信する。

【００１９】
次に、チャネル要求メッセージが、第１の移動切換制御局から第２のシステム内の第２の移動切換制御局に通信される。第２の基地局では、移動局から受信された信号の定量化可能パラメータもまた測定される。第２の基地局は、定量化可能パラメータの測定値が所定のレベルを越えると移動局との通信を確立する。あるいは、第１の基地局によって送信された第１のパイロット信号の信号強度が、移動局で測定される。次に、第１のパイロット信号の測定された信号強度が第２の所定のレベル未満であると、ハンドオフ要求メッセージが第２の基地局に送られ、よって移動局通信が確立される。移動切換制御局同士間に音声リンクを備えると、第１と第２のセルラーシステム間における既存の接続の送出が可能となり、また、システム間ソフトハンドオフの実行が可能となる。

【００２０】
双方のシステムがＣＤＭＡベースであり、双方が共にソフトハンドオフを実行可能である状況に対して、この装置が良好に働いている限り、これらシステムのうちの１つ以上がこのようなハンドオフを実行できないシステム間ハンドオフをどのように取り扱うかという問題が残る。例えば、いわゆるＧＳＭ基準には、ソフトハンドオフのメカニズムが存在しない。従って、エアインタフェースを用いてＣＤＭＡネットワークからＧＳＭネットワークに呼出しをハンドオフする際に問題がある。更に、ＧＳＭの認証に必要なデータをＣＤＭＡ２０００メカニズムは伝送することが不可能なため、ＧＳＭの認証は実行不可能である。ＧＳＭにおける暗号化は、ＣＤＭＡ２０００における暗号化とは異なる。

【００２１】
この問題を取り扱う１つの方法は、ＧＳＭを修正して、非ＧＳＭシステム、例えば、ＣＤＭＡシステムに対するハンドオフを達成させることを可能とすることである。しかしながら、ＧＳＭは今や長期にわたって確立されてきて、相対的に言って、オペレータは、隣の不適合のシステムに対応するために既存の装置に対して高価な修正を施そうとはしたがらない。デュアルモード移動局をサポートするに際、エアインタフェースに対して新たなメッセージが追加されると、これらの新たなメッセージをサポートするために、修正を実行しなければならない。率直に言って、これはオペレータの見解から言えば好ましくない。

【００２２】
ＣＤＭＡシステムとＧＳＭシステム間でハンドオフすることに伴う別の問題は、ＣＤＭＡとＧＳＭとの認証には２つの異なった方法と鍵とが用いられるという点である。ＧＳＭとＣＤＭＡ　１Ｘとにおける認証方法は基本的に同じであるが、鍵はサイズが異なっている。ＣＤＭＡ　１Ｘは、固有のチャンレンジ方法とカウント方法などの追加の手順があるが、これらはそれぞれ、チャネルのハイジャックと再生に対するアタックとを防止するものである。

【発明の開示】
【００２３】
［発明の概要］
本発明の一態様によれば、第１の移動切換制御局によって制御される第１のセルラー通信システム中の第１の基地局から第２の移動切換制御局によって制御される第２の別のセルラーシステム中の第２の基地局への暗号解読用鍵を移動局で用いる方法が提供されるが、前記方法は、前記第２のセルラー通信システム内での通信中に前記移動局によって用いられる暗号解読鍵を前記移動局に対して生成することであって、前記暗号解読鍵が、前記第２のセルラー通信システムに対する前記移動局に割り当てられた秘密鍵と前記第２のセルラー通信システムによって発生した乱数とから前記移動局によって生成されることと、前記暗号解読鍵を前記第１の移動局に通信することと、前記第１のセルラー通信システム内での通信中に前記移動局によって用いられる秘密長符号を前記移動局に対して生成することを備える。

【００２４】
本発明の別の態様によれば、第１のセルラー通信システム中の基地局と信号を送受信す

るように操作可能なトランシーバチェインと、第２のセルラー通信システムによって発生した乱数を受信し、前記セルラー通信システム内で通信中に前記移動局によって用いられる暗号解読鍵を前記移動局に対して生成するコントローラであって、前記暗号解読鍵が前記セルラー通信システムに対する前記移動局に割り当てられた秘密鍵と前記受信された乱数とから生成されるコントローラと、を備える移動局が提供される。

【００２５】

従って、本発明を実施するにあたって、ＧＳＭモバイルサービス切換センター（ＭＳＣ）を大幅に修正する必要なくＣＤＭＡ物理層をＧＳＭシステム内で使用することを可能とする１つの方法は、このＣＤＭＡ物理層に対するＧＳＭ認証方法を再使用することである。これによって、システムは、２つの異なったタイプの認証センターや、２つのタイプのＳＩＭカードなどをサポートする必要がないという長所が提供される。

【００２６】

本発明の上記の特徴と更なる特徴は、特に添付クレーム中に記載されており、また、その長所と共に、添付図面を参照して与えられる本発明の例示実施形態に関する以下の詳細な説明を考えればより明瞭となるであろう。

【発明を実施するための最良の形態】

【００２７】

図１は、例示のセルラー電話システムの概略図である。図示のシステムは、一般的に非常に多いシステム移動局又は移動電話と基地局との間の通信を実行し易くする様々な多元接続変調技術のうちのどれかを利用する。このような多元接続通信システム技術には、時分割多元接続方式（ＴＤＭＡ）、周波数分割多元接続方式（ＦＤＭＡ）、符号分割多元接続方式（ＣＤＭＡ）及び、振幅圧伸単側波帯などのＡＭ変調方式がある。例えば既に参照した米国特許第４，９０１，３０７号に開示されているＣＤＭＡのスペクトル拡散変調技術は、多元接続通信システムに対して他の変調技術にない重要な長所を有しており、従って、好ましいとされる。

【００２８】

一般的なＣＤＭＡシステムにおいては、各基地局が固有のパイロット信号を送信するが、この操作には、「パイロットキャリヤ」を対応するパイロットチャネル上で送信する操作が含まれる。このパイロット信号は、共通疑似ランダム雑音（ＰＮ）拡散符号を用いて各基地局によっていつでも送信される未変調で、直接シーケンスな、スペクトル拡散信号である。このパイロット信号によって、移動局は、コヒーレント復調のための位相基準と、ハンドオフの判定で用いられる信号強度測定値の基準とを提供することに加えて初期システム同期、すなわち、タイミングを得る。各基地局によって送信されたパイロット信号は、しばしば、同じＰＮ拡散符号であるが、符号位相オフセットは異なっている。

【００２９】

図１に示すシステムでは、モバイルスイッチングセンター（ＭＳＣ）とも呼ばれるシステムコントローラ／スイッチ１０は、一般的には、インタフェースと処理回路（図示せず）を含んでおり、これで、複数の基地局１２、１４及び１６に対してシステム制御を提供する。コントローラ１０はまた、適切な移動局に対して送信するための公衆交換電話網（ＰＳＴＮ）から適切な基地局への電話呼出しのルーティングを制御する。コントローラはまた、少なくとも１つの基地局を介してＰＳＴＮへの移動局からの呼出しのルーティングを制御する。このような移動局は一般には、互いに直接通信することはないので、コントローラ１０は、モバイルユーザ同士間の呼出しを適切な基地局を介して指揮する。

【００３０】

コントローラ１０は、専用電話回線、光ファイバリンク、マイクロ波通信リンクなどの様々な手段によって基地局にカップリングされていてもよい。図１では、３つのこのような例示の基地局１２、１４及び１６が、セルラー電話を含む例示の移動局１８と共に図示されている。矢印２０ａと２０ｂが、基地局１２と移動局１８間の可能な通信リンクを定めている。矢印２２ａと２２ｂが、基地局１４と移動局１８間の可能な通信リンクを定めている。同様に、矢印２４ａと２４ｂが、基地局１６と移動局１８間の可能な通信リンク

を定めている。

【００３１】

基地局サービスエリア又はセルは、移動局が通常１つの基地局に最も近くなるようにその地理的形状が設計されている。その移動局が空き局であると、すなわちどの呼出しも処理中でないと、移動局は常に、近傍の各基地局からのパイロット信号の送信を監視する。図１に示すように、パイロット信号は移動局１８に対して、基地局１２、１４及び１６によって、それぞれ通信リンク２０ｂ、２２ｂ及び２４ｂ上で送信される。次に、移動局は自分がどのセルの中にいるかを、これらの特定の基地局から送信されたパイロット信号の強度を比較することによって判定する。

【００３２】

図１に示す例では、移動局１８は、基地局１６に最も近いと考えられる。移動局１８が呼出しを開始すると、制御メッセージが最も近い基地局、ここでは基地局１６に送信される。呼出し要求メッセージを受信すると、基地局１６は、システムコントローラ１０に対してこのことを通知し、呼出し番号を転送する。すると、システムコントローラ１０は、呼出しを、ＰＳＴＮを介して意図される受信者に接続する。

【００３３】

呼出しがＰＳＴＮ内で開始されたとすると、コントローラ１０は呼出し情報をそのエリア中の全ての基地局に送信する。これらの基地局は、その返信にページングメッセージを、意図する受信者の移動基地局に送信する。移動局は、ページメッセージが聞こえたら、制御メッセージで応答し、このメッセージは最も近い基地局に送信される。この制御メッセージは、システムコントローラに対して、この特定の基地局が移動局と通信中であることを通知する。すると、コントローラ１０は、この呼出しを最も近い基地局から移動局にルーティングする。

【００３４】

移動局１８が最初の基地局、すなわち、基地局１６の有効範囲エリアから外に出ると、呼出しを別の基地局からルーティングすることによってその呼出しを継続しようと試行する。ハンドオフプロセスにおいては、呼出しのハンドオフを開始する又は別の基地局からルーティングする様々な方法が存在する。

【００３５】

基地局で開始されるハンドオフ方法では、最初の基地局、すなわち、基地局１６は、移動局１８によって送信された信号があるしきい値レベル未満に落ちるとそれに気付く。その時、基地局１６はハンドオフ要求をシステムコントローラ１０に送信し、このシステムコントローラは、この要求を、基地局１６の全ての隣接する基地局１２と１４に中継する。コントローラが送信する要求には、移動局１８によって用いられるＰＮ符号シーケンスを含むチャネルに関する情報が含まれている。基地局１２と１４は、移動局によって使用されているチャネルに対して受信器をチューニングして、一般的にはディジタル技術を用いて信号強度を測定する。基地局１２と１４の受信器のうちの一方が最初の基地局が報告した信号強度より強い信号を報告すると、その基地局にハンドオフされる。

【００３６】

あるいは、移動局自身がいわゆるモバイル支援式ハンドオフを開始する。基地局は各々がパイロット信号を送信し、この信号が、とりわけ、基地局を識別する。移動局は探索用受信器を備えており、これを用いて、他の機能を実行することに加えて、隣接する基地局１２と１４によるパイロット信号の送信をスキャニングする。隣接する基地局１２と１４のうちの一方の基地局のパイロット信号が所与のしきい値より強いことが分かった場合、移動局１８は現行の基地局１６に対してその旨のメッセージを送信する。

【００３７】

次に、移動局と基地局間の対話式プロセスによって、移動局は、基地局１２、１４及び１６のうちの１つを介して通信する。このプロセス中、移動局は、受信したパイロット信号を識別してその強度を測定する。この情報は、移動局が通信している基地局を介して、ＭＳＣに通信される。ＭＳＣは、この情報を受信すると、移動局と基地局間の接続を開始

したり終了したりして、モバイル支援式ハンドオフを達成させる。

【００３８】

このプロセスもまた、移動局が２つ以上の基地局を介して同時に通信するという点で「ソフトな」ハンドオフと考えられる。ソフトハンドオフ中は、ＭＳＣは、別々のセル同士間を移動している最中にモバイルユニットが通信している各基地局から受信された信号を合成したり選択したりすることが可能である。同様にして、ＭＳＣはＰＳＴＮからの信号を、モバイルユニットが通信している各基地局に中継する。モバイル支援式ハンドオフは、移動局が同じセルラーシステム内にはない２つ以上の基地局の有効範囲エリア内にあったりするとより複雑になる、すなわち、同じＭＳＣでは制御されない傾向がある。

【００３９】

互いに異なったシステム内の基地局同士間でハンドオフを実行する１つの方式を、ＣＤＭＡモバイルスイッチングセンターＭＳＣｃの制御下にあるＣＤＭＡセルラーシステム（例えばＩＳ－９５　１Ｘ）とＧＳＭモバイルスイッチングセンターＭＳＣｇの制御下にあるＧＳＭセルラーシステムとが含まれるセルラー通信ネットワーク３０を略式で示す図２を参照して以下に説明する。図２に、ＧＤＭＡシステムのセルＣ１Ａ～Ｃ５Ａ内にそれぞれ置かれている５つのこのような例示の基地局Ｂ１Ａ～Ｂ５Ａ、及びＧＳＭシステムのセルＣ１Ｂ～Ｃ５Ｂ内にそれぞれ置かれている５つの基地局Ｂ１Ｂ～Ｂ５Ｂを示す。図示しやすいように、セルＣ１Ａ～Ｃ５Ａ及びＣ１Ｂ～Ｃ５Ｂを円形で示しているが、セルは一般には他の形状であるように設計され、実際、自身が置かれているエリアの地形とトポグラフィによって異なる形状を有することを理解すべきである。セルＣ１Ａ～Ｃ３ＡとＣ１Ｂ～Ｃ３Ｂの後に続くセルは「境界」(border)セルと呼ばれるが、それは、これらのセルは第１と第２のセルラーシステム間の境に近接しているからである。このように指名することによって、各システム内の残余のセルを「中間」(internal)セルと呼ぶと便利である。

【００４０】

ＣＤＭＡセルラーシステムとＧＳＭセルラーシステム双方内の基地局からの信号を受信してこれに反応することが可能な移動局を参照して以下に説明する。しかしながら、ＣＤＭＡ　１、ＣＤＭＡ２０００、ＣＤＭＡ２０００　１ｘ、ＣＤＭＡ　２０００　３ｘ、高データレート方式（ＨＤＲ）、ＣＤＭＡ　１ｘＥＶ、ＣＤＭＡ　１ｘＥＶＤＯ、ＴＤＭＡ、ＴＤＳＣＤＭＡ、Ｗ－ＣＤＭＡ、ＧＰＲＳ及びその他などの通信システムのうちのどれでも用いられることが熟慮される。この目的のため、移動局を、２個のセルラーシステムの様々な操作周波数に対してチューニング可能な受信チェインを有するデュアル帯域トランシーバで構成する。このような移動局の概略図を添付図面の図３に示す。そこに示すように、移動局４０は、ダイプレクサ４４を介してＣＤＭＡ送受信チェイン４６とＧＳＭ送受信チェイン４８の双方に接続されているアンテナ４２を備えている。送／受信チェイン４６と４８は、従来から、それぞれＣＤＭＡシステムとＧＳＭシステムに対応している。これらのチェインは、適切に復調され変換されたデータを従来のベースバンド回路５０に出力して、ベースバンド回路４０からの送信用データを受信する。送／受信チェイン４６と４８はコントローラ５２によって制御されるが、このコントローラは、とりわけ、ＣＤＭＡシステム又はＧＳＭシステムからのコマンド信号に応答してこれら２つのチェインを切換える。従って、本実施形態では、これら２つのチェインは同時にアクティブにはならない。別の実施形態では、これら２つのチェインは同時にアクティブとなる。

【００４１】

別の実施形態では、移動局は、これら２個のセルラーシステムのうちの一方に対してチューニング可能な受信チェインを有する単一のトランシーバで構成される。このような移動局の概略図を、添付図面の図５に示す。この図に示すように、移動局５３はアンテナ５４を備えている。ダイプレクサ５５は、ＣＤＭＡ送受信チェイン５６に（それがＣＤＭＡハンドセットであれば）接続される。そうでなければ、移動局５３はＧＳＭ送受信チェイン５７に接続される。送／受信チェイン５６と５７は、従来から、それぞれＣＤＭＡシステムとＧＳＭシステムに対応している。このチェインは、適切に復調され変換されたデー

タを従来のベースバンド回路５８に出力して、ベースバンド回路５８からの送信用データを受信する。送／受信チェインは、５６又は５７がコントローラ５９によって制御される。

【００４２】

図２に戻ると、ＣＤＭＡモバイルスイッチングセンター（ＭＳＣｃ）は、公衆交換電話網（ＰＳＴＮ）からの適切な基地局Ｂ１Ａ～Ｂ５Ａへの電話呼出しの、指定された移動局に送信するためのルーティングを制御している。ＣＤＭＡモバイルスイッチングセンターＭＳＣｃはまた、第１のセルラーシステムの有効範囲内の基地局からの少なくとも１つの基地局を介してのＰＳＴＮに対する呼出しのルーティングを制御する。ＧＳＭモバイルスイッチングセンターＭＳＣｇは同様に操作して、基地局Ｂ１Ｂ～Ｂ５Ｂの操作を統御し、また、ＰＳＴＮとＧＳＭセルラーシステム間で呼出しをルーティングする。制御メッセージなどはＭＳＣｃとＭＳＣｇ間でシステム間データリンク３４を介して通信される。

【００４３】

移動局がＣＤＭＡシステムの中間セル内に位置している場合、移動局は、一般的には、各近傍（すなわち、中間及び／又は境界）基地局からのパイロット信号の送信を監視するようにプログラムされる。すると、移動局は、周辺の基地局から送信されたパイロット信号強度を比較することによってどの中間セル中に自分が位置するか判定する。移動局が中間セルの境界に接近すると、モバイル支援式ハンドオフが、例えば、米国特許第５，２７６７，２６１号を参照して上述したように開始される。

【００４４】

移動局が境界セルＣ１Ａ～Ｃ３Ａ又はＣ１Ｂ～Ｃ３Ｂのうちの１個のセル内に置かれるような別の状況が存在する。例として、移動局がセルＣ２Ａ内に置かれているがセルＣ２Ｂに接近している場合を考えてみる。この例では、移動局は、基地局Ｂ２Ｂから使用可能な信号レベルを受信し始めることが可能であり、次にこれが、移動局が現在通信中の基地局Ｂ２Ｂと他のどれかの基地局に報告される。使用可能な信号レベルが移動局又は基地局によって受信されている時刻は、受信された信号の１つ以上の定量化可能なパラメータ（例えば、信号強度、信号対雑音比、フレーム消去レート、ビットエラーレート及び／又は相対的遅延時間）を測定することによって決定される。このメカニズムは上記の確認された米国特許第５，６９７，０５５号に記載されているメカニズムと類似している。

【００４５】

双方のシステムがＣＤＭＡシステムである場合、米国特許第５，６９７，０５５号に記載のハンドオフメカニズムは、セルＣ２Ａとセル Ｃ２Ｂ間のハンドオフを達成させるために用いることが可能である。しかしながら、エアインタフェースを用いてＣＤＭＡネットワークからＧＳＭネットワークに呼出しをハンドオフするメカニズムが現時点では存在しないという問題がある。ＧＳＭ認証は、ＧＳＭ認証に必要とされるデータをＣＤＭＡメカニズムが転送できないため実行不可能である。ＧＳＭ内での暗号化はＣＤＭＡ内での暗号化とは異なっている。新しいメッセージが、デュアルモード移動局のサポートに際してエアインタフェースに追加されると、これらの新しいメッセージをサポートするために修正を施さなければならない。これは望ましくない。

【００４６】

この問題に対する解決策は、移動局によるＣＤＭＡネットワークからＧＳＭネットワークへの転送を可能とさせる命令を含む一般的メッセージを用いることである。この一般的メッセージは、ＧＳＭの認証と暗号化を達成させるために必要とされるデータを転送することが可能でなければならない。ＧＳＭ中の他の補足的特徴もまた、一般的メッセージでサポートすべきであるとされるのが望ましい。言い換えれば、確立されたＧＳＭプロトコルは無傷のまま保持し、これで、既存のＧＳＭシステム中のいかなる変更をも最小化するようにしなければならない。ハンドオフ操作の一部には、加入者の身元を確立する操作が含まれており、一旦ハンドオフが達成されたら、物理的接続暗号化のためのシグナリングとデータ秘密性とを維持することが必要となる。加入者の身元の認証の定義と操作要求とはＧＳＭ０２．０９に規定されている。

【００４７】
この認証の手順もまた、暗号解読用鍵を設定するために用いられる。従って、この認証手順は、ネットワークが加入者の身元を確立した後でしかもチャネルが暗号化される以前に実行される。２つのネットワーク機能が、これを達成するために必要である。すなわち、認証手順自身とこのシステム内での認証鍵と暗号化鍵との管理である。
【００４８】
これを念頭において、いつでも（ハンドオフ状況と非ハンドオフ状況）作動し、また、単方向性又は双方向性であるトンネルメカニズムの利用を考慮する。１つのタイプのトンネルメカニズムは、一般的にはＧＳＭ基地局コントローラ（ＢＳＣ）によって検査されないがデュアルモード移動局によって必要とされるＣＤＭＡシステムのＧＳＭパラメータ内を透明性をもって通過するいわゆるＡＤＤＳ（アプリケーションデータ送出サービス）メッセージと短データバーストメッセージとのことである。ＡＤＤＳメッセージをデータバーストと共に用いると、上記のネットワーク又は他のネットワークエレメント（例えば、ＳＭＳ、位置ロケーションサーバ、ＯＴＡＳＰ）のモバイルサービススイッチングセンター（ＭＳＣ）同士間で一般ペイロードを送ることが可能となる。本システムは、これを利用して、ＧＳＭ情報をエンド・ツー・エンドでネットワークと移動局との間で、ＣＤＭＡのＢＢＳ又はＢＴＳｃに対して何ら変更を加える必要なく通過させる。
【００４９】
図２に示すネットワーク構造では、ＡＤＤＳメッセージを用いて、タイミング情報や認証データなどのＧＳＭハンドオフデータをＭＳＣｃからＢＳＣｃを介して移動局に転送する。すると、この移動局はいわゆるＭＡＰ（モバイルアプリケーションプロトコル）メッセージを用いて、このハンドオフデータをＧＳＭネットワーク中のＭＳＣｇに転送する。これには、ＭＳＣｇに少し変更を加えて、ＭＡＰメッセージ中のデータを解釈して、それに従って移動局を制御する必要がある。データを転送する他の代替例も、もちろん可能である。
【００５０】
移動局がＣＤＭＡシステムとＧＳＭシステム間の境界にある（例えば、セルＣ２Ａ中にあるがセルＣ２Ｂに接近している）場合、移動局は、モバイルがＧＳＭシステムに対してハンドオフされるべきであるような条件下にあることをＭＳＣｃに通知するメッセージをＭＳＣｃに送り返すことによってハンドオフプロセスを開始する。
【００５１】
セルデータベース（図示せず）が、ハンドオフ手順の一部として用いられる。このデータベースを用いて、ＧＳＭネットワークに関する必須の情報をモバイルに提供し、従って、ＣＤＭＡのＭＳＣとＧＳＭとの間でのハンドオフを必要に応じて実行することが可能となる。
【００５２】
ＧＳＭシステムでは、２つのタイプのハンドオフが利用可能である。すなわち、同期式ハンドオフと非同期式ハンドオフである。実施しやすいように、非同期式ハンドオフが好ましい。従って、移動局は、ハンドオフはＧＳＭに対する非同期式ハンドオフであることを告げられる。ハンドオフ命令が移動局によって受信されたら、モバイルは最初に、ＧＳＭ認証データの生成を可能とするためにＣＤＭＡ　ＭＳＣｃに戻されて移動局に提供されたＭＡＰハンドオフメッセージが戻ってきてそれを受信するまで、いくつかのアクセスバーストをＧＳＭ基地局コントローラＢＳＣｇに対して送る。ＧＳＭは非同期式ハンドオフの手順を有し、データバーストは、ＢＳＣｇがモバイルに対するタイミングを獲得するのを助ける。従って、ＡＤＤＳメッセージには、ハンドオフが生成する特定の時刻を指定する「反応時間」が含まれる。一旦このデータが受信されただけで、モバイルは通常の送信を開始する。
【００５３】
ＣＤＭＡとＧＳＭ間でのハンドオフに伴う別の問題は、ＣＤＭＡとＧＳＭの認証には２つの異なった方法と鍵が用いられるということである。このＧＳＭとＣＤＭＡ　１Ｘにお

ける認証方法は基本的には同じであるが、鍵はサイズが異なっている。ＣＤＭＡ　１Ｘは、それぞれチャネルのハイジャックと再生攻撃を防止する固有チャレンジ方法とカウント方法などの追加の手順を有する。ＧＳＭ　ＭＳＣｇに対して大幅な修正を必要とすることなくＣＤＭＡ物理層をＧＳＭシステム内で用いるためには、ＧＳＭ認証方法をＣＤＭＡ物理層に対して再使用すべきである。これによって、システムが互いに異なった２つのタイプの認証センター、２つのタイプのＳＩＭカードなどをサポートする必要がないという長所が提供される。

【００５４】

この認証手順は、システムと移動局間での一連の交換動作から構成される。本システムは予測不可能番号ＲＡＮＤを移動局に送信する。次に、移動局は、ＲＡＮＤ番号の署名としても知られる結果ＳＲＥＳを、Ａ３アルゴリズムとして知られているアルゴリズムを用いて計算する。Ａ３アルゴリズムは、ＲＡＮＤと個別加入者認証鍵Ｋｉとを用いて、ＳＲＥＳを計算する。加入者認証鍵Ｋｉは、顧客が最初にサービスに加入して、本システムのＳＩＭ（契約者固有モジュール）カードとホームロケーションレジスタ（ＨＬＲ）の双方に記憶されると割り当てられる。Ｋｉは、暗号化における秘密鍵であり、従って、決してネットワーク上で送信されることはない。最後に、移動局は署名ＳＲＥＳをシステムに送信し、そこで、有効であるかどうか試験される。

【００５５】

暗号解読用鍵の記述された用法と認証手順は、ハンドオフプロセスとは無関係であることに注意すべきである。添付図面の図４に、ＧＳＭ　ＭＳＣ中でどのように認証を達成させるかを示す。ＧＳＭ中の認証鍵はＫｉと呼ばれ、その長さは１２８ビットである。ネットワークは乱数（ＲＡＮＤ）を発生するが、これも１２８ビット長である。ＲＡＮＤとＫｉは、Ａ３アルゴリズムに入力され、このアルゴリズムは入力データから３２ビットの結果（ＳＲＥＳ）を計算する。ＲＡＮＤ番号もまた、移動局に対して、エアメッセージを介して送信される。ＧＳＭシステムでは、各移動局がスマートカード、すなわち、いわゆるＳＩＭ（契約者固有モジュール）カードを含んでいる。認証用の標準のＳＩＭコマンドはＧＳＭ１１．１１に指定されている。これらのコマンドは、ＧＳＭアプリケーションの正しい機能を妨げない場合に実行することが許されるだけである。ＳＩＭが呼出し中に移動局から取り除かれると、ＧＳＭ１１．１１に定められているように、その呼出しは即座に終了される。

【００５６】

移動局中のＳＩＭもまた、受信したＲＡＮＤ番号とローカルで記憶されているＫｉのコピーとにＡ３アルゴリズムを適用することによってＳＲＥＳを計算する。この計算結果はこれまたＳＲＥＳであり、ネットワークによって計算されたＳＲＥＳと同じであるはずである。従って、結果ＳＲＥＳは移動局によってネットワークに送られ、ここで、ネットワークが計算したＳＲＥＳの値と比較される。双方のＳＲＥＳ値が同じであれば、移動局は認証される。図２のシステムでは、ＲＡＮＤ番号は、エアインタフェース上でＡＤＤＳメッセージを用いて送信され、結果ＳＲＥＳは送信されて戻される。

【００５７】

ＳＲＥＳの値もまた、Ａ８として知られているアルゴリズム中で用いられて、６４ビットの暗号化鍵又は暗号解読用鍵Ｋｃを計算する。移動局中でＳＩＭによってＧＳＭ認証アルゴリズムと暗号化アルゴリズムを用いて生成されたＫｃ鍵は、通常はＣＤＭＡ　ＣＡＶＥアルゴリズムを用いて生成される秘密長符号マスクの代わりにＣＤＭＡ物理層に適用される。この６４ビットＫｃ鍵は、４２ビット秘密長符号に対して固有にマッピングされ、従って、「秘密長符号マスク」の基礎として用いられて、音声プライバシを提供する。この秘密長符号マスクは、ＣＤＭＡメッセージに伴って送付され、ＣＡＶＥアルゴリズムに基づいて生成された場合と全く違いがないように解釈される。音声プライバシのためのこの方法を用いると、本システムは、ハイブリッドＣＤＭＡ／ＧＳＭネットワーク内で固有の認証センターと固有のＳＩＭタイプとを保持することが可能である。

【００５８】

ＧＳＭはフレームレベルで暗号化を実行する。全てのフレームは、フレーム番号と６４ビットのＫｃ鍵を用いて暗号化されるが、この鍵は図４を参照して説明したように誘導される。フレーム番号とＫｃマスクは全てのフレームに適用される。ＣＤＭＡ　１Ｘシステムでは、暗号化は４２ビットの秘密長符号を用いて実行される。図２のハイブリッドシステムでは、Ｋｃ鍵を用いて４２ビット秘密長符号マスクを誘導するが、マッピングアルゴリズムがＫｃと秘密長符号間でマッピングする。このマッピングはＭＳＣｃ中で実行され、次に、ＭＳＣｃはＢＳＣに対して、どの秘密長符号を用いるべきであるか告げる。

【００５９】

ＡＤＤＳ操作によって、地上ネットワークエレメント（例えばＭＳＣ、ＳＭＳ、ＰＤＣ）と移動局との間での透明なサービスの転送が許容される。本システムはこの操作を用いて、認証情報ＲＡＮＤをＭＳに転送し、また、ＳＲＥＳをＭＳＣに転送して返す。ＡＤＤＳメッセージング操作はＭＳＣｃからＢＳＣｃに移行し、これで、データを移動局に対してページングチャネルを介して送ることができる。ＡＤＤＳ転送操作はＢＳＣｃからＭＳＣｃに移行し、これで、データを移動局からネットワークに対してアクセスチャネルを介して送ることができる。ＡＤＤＳ送出操作はＭＳＣｃからＢＳＣｃ又はＢＳＣｃからＭＳＣｃに移行し、これで、データを移動局とネットワーク間でトラフィックチャネルを介して送ることができる。ＡＤＤＳパラメータは「ＡＤＤＳユーザパート」として定義されているが、これは、アプリケーションデータメッセージの形式を示す６ビットの「データバーストタイプ」を含んでいる。ＡＤＤＳ操作はＡＤＤＳユーザパートパラメータを利用して、サーバ別のデータを包含する。認証動作はＡＤＤＳユーザパートを利用して、認証データを搬送する。ここに説明するシステムは「ＧＳＭ－ＭＡＰ認証」という名称の新しいデータバーストタイプを用いるが、これは従って、移動局によって解釈される。

【００６０】

この例示の実施形態は、認証プロセスに関連する情報を記憶するデータベースが受信端に存在する、又は、受信端によってアクセス可能であるときはいつでも実施されることに注意すべきである。この例示の実施形態のプロセッサを用いて、１つの当事者での１つの暗号方式と別の当事者での別の暗号方式を実施する。この例示の実施形態の基本的な実施例は、中間のリソースに対して物理的に接続する必要なく実施されるが、それは、別々の当事者との通信が無線媒体を介して生成するからである。

【００６１】

当業者は、本明細書に開示する実施形態と関連して説明した様々な解説的な論理ブロック、モジュール、回路及びアルゴリズムステップは、電子式ハードウエア、コンピュータソフトウエア又は双方の組み合わせとして実現されることが理解されよう。これら様々な解説的なコンポーネント、ブロック、モジュール、回路及びステップを、概してその機能性という点について説明した。この機能性がハードウエアとして実現されるかソフトウエアとして実現されるかは、特定の応用とシステム全体に課せられる設計上の制限とによって決まる。当業者は、このような環境下ではハードウエアとソフトウエアが交換可能であることや特定の応用毎に記述の機能性をどのように実施したら最良であるかが認識されよう。例として、本明細書に開示する実施形態に関連して説明した様々な解説的な論理ブロック、フローチャート、ウインドウ及びステップはハードウエアやソフトウエアとして実現又は実施されるが、その際に用いられるのは、特定用途向け集積回路（ＡＳＩＣ）、プログラマブル論理デバイス、ディスクリートゲートもしくはトランジスタロジック、ディスクリートハードウエアコンポーネント、例えばＦＩＦＯ中のレジスタ、ファームウエア命令の集合を実行するプロセッサ、何らかの従来型のプログラム可能なソフトウエア及びプロセッサ、フィールドプログラム可能ゲートアレイ（ＦＰＧＡ）もしくは他のプログラム可能ロジックデバイス又はこれらの組み合わせなどである。このプロセッサは、マイクロコントローラであれば長所となるが、代替例では、プロセッサは何らかの従来型プロセッサ、コントローラ、マイクロコントローラ又は状態機械である。このソフトウエアは、ＲＡＭメモリ、フラッシュメモリ、ＲＯＭメモリ、ＥＰＲＯＭメモリ、ＥＥＰＲＯＭメモリ、ハードディスク、取り外し可能ディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、レジスタ

又は他の何らかの磁気式もしくは光学式記憶媒体上に常駐する。当業者は、更に、上記の説明全般にわたって参照したデータ、命令、コマンド、情報、信号、ビット、記号及びチップは、電圧、電流、電磁波、磁場もしくは磁粒子、光場もしくは光粒子又はこれらの組み合わせで表せば長所となることが理解されよう。

【００６２】

本発明を好ましい実施形態を参照して説明したが、当該実施形態は単なる例示であり、また、適切な知識と熟練の所有者には思い当たるような修正及び変更が添付クレーム及びその等価物に記載される本発明の精神と範囲から逸脱することなく実施されることがよく理解されよう。

【図面の簡単な説明】

【００６３】

【図１】セルラーシステムの概略図である。

【図２】２個のセルラーシステム間の境界の概略図である。

【図３】デュアルモード移動局の概略図である。

【図４】ＧＳＭシステムにおけるデータ交換の概略図である。

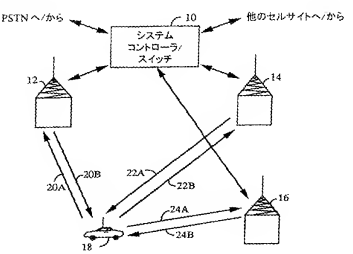
【図５】単一モードの移動局の概略図である。

【符号の説明】

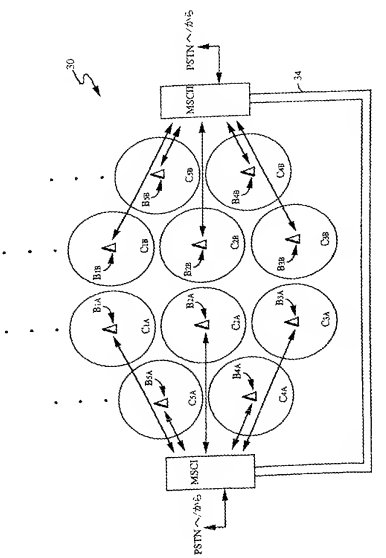
【００６４】

１０…システムコントローラ／スイッチ、１２，１４，１６…基地局、１８…移動局、２０ａ－２０ｂ，２２ａ－２２ｂ，２４ａ－２４ｂ…通信リンク、３４…システム間データリンク、４０…移動局、４２…アンテナ、４４…ダイプレクサ、４６…ＣＤＭＡ送受信チェイン、４８…ＧＭＳ送受信チェイン、５０…ベースバンド回路、５２…コントローラ、５３…移動局、５４…アンテナ、５５…ダイプレクサ、５６…ＣＤＭＡ送受信チェイン、５７…ＧＳＭ送受信チェイン、５８…ベースバンド回路、５９…コントローラ

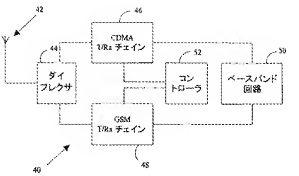
【図１】



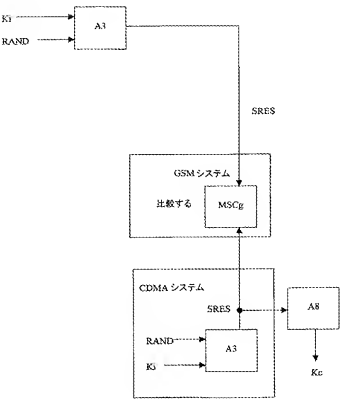
【図２】



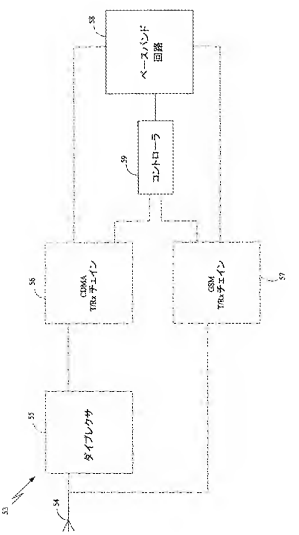
【図３】


42
46
CDMA
T/Rx チェイン
44
52
50
ダイ
プレクサ
コン
トローラ
ベースバンド
回路
GSM
T/Rx チェイン
40
48

【図４】


Ki
RAND
A3
SRES
GSM システム
比較する
MSCg
CDMA システム
SRES
A8
RAND
A3
Ki
Kc

【図５】


58
ベースバンド
回路
59
コントローラ
56
CDMA
T/Rx チェイン
GSM
T/Rx チェイン
57
55
ダイプレクサ
53
54

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/39209

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04Q 7/20,7/38
US CL : 455/422,432, 436,437,438,439,440,517
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/422,432, 436,437,438,439,440,517

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/0146127 A1 (WONG) 10 October 2002, see fig. 3b, paragraph 0043 through paragraph 0050.	1,2,4-13,15,16
A	US 5,778,075 A (HAARTSEN) 07 July 1998, see fig. 1 numbers 30,14 and 20, col. 4 lines 51-67.	1,6,8,12
A	US 2002/0091933 A1 (QUICK, JR et al.) 11 July 2002, see abstract.	1-16

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 January 2003 (16.01.2003)	07 MAR 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Keith Ferguson Telephone No. (703) 305-4888

Form PCT/ISA/210 (second sheet) (July 1998)

フロントページの続き

(31)優先権主張番号 60/358,491
(32)優先日 平成14年2月19日(2002.2.19)
(33)優先権主張国 米国(US)

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 ホルクマン、アレジャンドロ・アール
アメリカ合衆国、カリフォルニア州 ９２１０７、サン・ディエゴ、デモンシャー・ドライブ １０５４
(72)発明者 ジャイン、ニクヒル
アメリカ合衆国、カリフォルニア州 ９２１３０、サン・ディエゴ、フェダーマン・レーン ４２９１
(72)発明者 ハンター、アンドリュー・ティー
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５

Fターム(参考) 5J104 AA01 AA16 AA32 EA01 EA04 EA15 EA16 JA03 MA07 NA02
NA37 PA01
5K067 AA30 BB04 BB21 CC04 CC10 DD17 DD45 DD51 DD57 EE04
EE10 EE16 GG22 HH21 HH36